AO 91 (Rev. 02/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of New York

United States of America)
v.)
)
Daniel C. Beal)
)
Defendant

Case No. 5:15-MJ-292 (ATB)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of _____ in the county of Oneida in the Northern District of New York, the defendant violated 18 U. S. C. § 2252A(a)(2)(A), an offense described as follows:
Between on or about August 2010 and on or about July 2015 did knowingly receive child pornography using a means and facility of interstate and foreign commerce in and affecting such commerce.

This criminal complaint is based on these facts:

See attached Affidavit.

☑ Continued on the attached sheet.

Complainant's signature

Alix Skelton, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 07/29/2015

Judge's signature

City and state: Syracuse, New York

Hon. Andrew T. Baxter, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT

I, Alix Skelton, a Special Agent with Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Federal Bureau of Investigation (FBI) Special Agent and have been employed in that capacity since December 2011. I am currently assigned to the Albany Division, Syracuse Resident Agency in Syracuse, New York. I have been involved in investigations and received training on a variety of criminal violations including the sexual exploitation of children and specifically violations of Title 18, United States Code, Section 2252A. I have been the affiant on several investigations involving violations of 2252A.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute search warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for a criminal complaint charging Daniel Beal with violations of Title 18, United States Code, Section 2252A(a)(2)(A) (receiving child pornography).

4. The information contained in this affidavit is based upon information gathered by me as a part of the investigation as well as information provided to me by other Special Agents of the FBI and other law enforcement officers involved in this investigation. Since this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish

probable cause to believe that Daniel Beal has committed violations of Title 18, United States Code, Section 2252A(a)(2)(A), as outlined above.

5. At all times throughout this affidavit I use the term "child pornography" to refer to visual depictions of actual minors engaged in sexually explicit conduct. I use the terms "visual depiction", "minor", and "sexually explicit conduct" as those terms are defined in 18 U.S.C. § 2256 (see DEFINITIONS section below).

Peer to Peer

6. Peer to peer (P2P) file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files currently being shared on the network. Ares, one type of P2P software, sets up its searches by keywords. The results of a keyword search using the Ares software are displayed to the user in the Ares program. The user then selects file(s) from the results for download to the user's computer. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) sharing the file. Typically, the file, once downloaded by the user, is made available for dissemination to other users of the Ares P2P software.

7. For example, a person interested in obtaining child pornographic images would open the P2P application on his/her computer and conduct a keyword search for files using a

term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed the file(s) he/she wants to download. The file is downloaded directly from the computer sharing the file. The downloaded file is stored in the area previously designated by the user and/or the software. The downloaded file will remain in that location until moved or deleted by the user.

8. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, on one P2P network, Ares, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often however, a user downloading a file receives the entire file from one computer.

9. The Ares P2P network bases all of its file shares on the Secure Hash Algorithm (SHA1). SHA1 is a mathematical algorithm that allows for the fingerprinting of files. Once a file is checked with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that value will be a fixed-length unique identifier for that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA1 is called secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.

10. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a

particular computer during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers.

11. The computer running the file sharing application, in this case Ares, has an IP address assigned to it while it is on the Internet. Investigators are able to see the IP address of any computer system sharing files. Investigators can then search public records that are available on the Internet to determine the Internet service provider who has assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the ISP. The following are facts known regarding the Ares file sharing network:

12. The Ares network is an open source public file-sharing network. Most computers that are part of the Ares network are referred to as nodes. A node can simultaneously provide files to some peers while downloading files from other nodes. Nodes may be elevated to temporary indexing servers referred to as "supernodes." Supernodes increase the efficiency of the Ares network by maintaining an index of the contents of network peers. Ares users query supernodes for files and are directed to one or more peers sharing that file. There are many supernodes on the network; accordingly, if one shuts down the network continues to operate.

13. The Ares network can be accessed by computers running many different client programs, some of which include the original Ares Galaxy program, and derivatives compiled from the source code, which is open source and freely available. These programs (a/k/a "clients") share common protocols for network access and file sharing. The user interface, features and configuration may vary between clients and versions of

the same client. In this case, the user was using a version of Limewire to access the network.

14. During the installation of an Ares client, various settings are established which configure the host computer to share files. Depending upon the Ares client used, a user may have the ability to reconfigure some of those settings during installation or after the installation is completed. Typically, a setting establishes the location of one or more directories or folders whose contents (files) are made available to other Ares users to download. This location is commonly referred to as the "My Shared Folder" or, colloquially, the "shared folder." In many versions of Ares clients, the shared folder defaults to appear on the computer's desktop.

15. The client software processes files located in a user's shared directory. As part of this processing, a SHA1 hash value is computed for each file in the user's shared directory. The client software processes files located in a peer's shared directory. As part of this processing, a SHA-1 hash value is loaded from a prior record or computed for each file in the user's shared directory.

16. The Ares network uses SHA-1 values to improve network efficiency. Users may receive a selected file from numerous sources by accepting segments of the file from multiple users and then reassembling the complete file on the local computer. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. The network uses SHA-1 values to ensure exact copies of the same file are used during this process.

17. Upon connecting to the Ares network, a list of shared files, descriptive information and the files associated SHA-1 values are sent to the supernodes. This allows other users to

locate these files. The frequency of updating information is dependent upon the client software being used and the Ares networking protocols. This information sent to the supernodes is only data about the file and not the actual file. The file remains on the user's computer. In this capacity, the supernode acts as a pointer to the files located on a user's computer.

18. When a download of a file is initiated, the user is presented with a list of users (nodes) who had told the Ares network that they have the requested file available for others to download. Typically, the supernodes and hosts computers on the network return this list containing node information and the IP addresses of computers which have reported they have the same file (based on SHA-1 comparison) or in some instances portions of the same file available to others to download. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known actual child pornography.

19. Obtaining files from the Ares network, as described herein, returns the candidate list, including IP addresses, which can be used to identify the location of computers. Although the IP address is not usually visible to the end user in the common Ares clients, it is returned and used by the software to initiate the download. Law Enforcement has modified the Ares program to allow the downloading of a file from a single IP address as well as displaying the IP address which is known to all Ares clients, but not typically displayed within the Ares clients.

OVERVIEW OF THE INVESTIGATION

20. On March 23, 2015, FBI SA Heather Weber was given information from the FBI Buffalo Field Office that an undercover Task Force Officer (TFO) had, on two separate

dates, successfully downloaded files shared from the Ares network from a computer at IP address 64.65.206.37. SA Weber reviewed these files, and they are available for the Court's review upon request.

A. On September 24, 2014 between 3:03 pm and 3:14 pm, the undercover TFO downloaded two video files from IP 64.65.206.37, which are described as follows:

1. A file titled (pthc) sally-my daughter at 5 (fucking little girl)(hardcore)(2).mpg, is a video file depicting a prepubescent female child being vaginally penetrated by an adult male, who is lying behind her.

2. A file titled (yamad)hussyfan(pt)';'1hannah-forced h319(2)(2).mpg, is a video file depicting a prepubescent female child positioned in a chair by an adult male to get a close- up video image of her vagina and anus.

B. On October 15, 2014 between 12:29 pm and 12:36 pm, the undercover TFO successfully downloaded a file being shared by a computer at IP address 64.65.206.37. This is an image file depicting a naked prepubescent female lying on her back, with a naked prepubescent boy between her legs. What appears to be an Asian adult male is depicted standing near the boy, pointing at the girl's vagina.

C. On July 20, 2015 the undercover TFO was able to access the Ares network and review the videos and images available for download and sharing in the shared folder for IP address 64.65.206.37. This program allows the TFO to see the hash value, IP address and city location of users on the Ares network. The TFO was able to see that the user of this IP address has been an active user on Ares since 2011 and has been on the Ares network consistently over the past two weeks including on July 20, 2015. The TFO was also able to identify by hash value 156 files with known child pornography images

and videos available for sharing by a computer at IP address 64.65.206.37 on July 20, 2015. Those files include:

1) An image depicting a pubescent female straddling an unknown male with his penis penetrating her vagina. This file is known child pornography that is part of the "Photo by Carl" series;

2) A video that is 2 minutes and 2 seconds in length that shows a nude prepubescent female lying on her back with her knees pulled up exposing her anus and vagina. The female exposes her vagina to the camera and an adult male masturbates over her vagina until he ejaculates on the female's vagina and lower abdomen; and

3) A video file named (pthc)(orgasm) 6yr 8yr and 11 yr-encoded by sw!tch(2).avi that is 17 minutes and 35 seconds long. The video depicts a nude prepubescent female masturbating.

The TFO was unable to download any of the videos and images on July 20, 2015 because the program is limited by the number of open connections to the user available at the time it is reviewing those files. In essence the program got a busy signal when trying to download on July 20, 2015 as the ports available for sharing were all being used at the time.

21. On March 17, 2015, and July 20, 2015, FBI SA Kimberly Williams served a subpoena on EarthLink, for records for the registered owner of the IP address 64.65.206.37. On March 20, 2015, and July 21, 2015, EarthLink provided the following subscriber information:

Dacobe Enterprises LLC
325 Lafayette St
Utica, NY 13502
Point of Contact: Geoff Thorp, phone number 315-XXX-XXXX[redacted]

The information provided in the subpoena return also indicates that this IP address has been registered to Dacobe Enterprises LLC since October 15, 2010. The United States Postal Service has confirmed that the address receives mail for only one business, Dacobe Enterprises LLC, and two individuals Daniel Coby Beal, and his partner "Geoff."

SEARCH WARRANT

On today's date, your affiant and other law enforcement officials went to Dacobe Enterprises LLC and executed a search warrant that had been authorized by the Hon. Andrew T. Baxter on July 21, 2015. BEAL was present at the time agents arrived to execute the search warrant. During a forensic preview of a hard drive BEAL identified as one used by him, FBI CART analyst Jude Kaiser located approximately 174 video files in a subfolder labeled "YG" that was located in a folder labeled "Vid" that appear to be consistent with child pornography. Your affiant has reviewed 6 of the video files. All 6 depict child pornography, and are available for the Court's inspection upon request. Those video files include:

1) A video dated May 8, 2015 titled 3001.wmv which is 2 minutes 11 seconds in length and depicts 2 females children approximately ages 2 and 4 years old manually stimulating an adult penis and the penetration of one of the vagina of one of the children by an adult male's penis;

2) A video dated May 8, 2015 titled 3011.mpg which is 7 minutes 2 seconds in length and depicts a female toddler of about 2 years in age whose vagina is being spread apart by an adult male to expose it to the camera. The male also uses his fingers to touch the child's vagina;

3) A video dated June 9, 2015 titled 10030.mpg which depicts an adult male engaging in penis to vagina contact with a prepubescent female child and the child manually stimulating the adult penis;

4) A video dated June 9, 2015 titled 10039.wmv which is 8 minutes 6 seconds in length and begins with text that reads "Manuela 9yr with daddy" which is a slideshow of pictures depicting a pre-pubescent female child whose age is consistent with the text engaging in mouth to penis contact with an adult male, and the penetration of the child's vagina with the adult's penis and a foreign object;

5) A video dated July 14, 2015 titled 20010.mpg which is 1 minute 11 seconds in length and depicts an adult male engaging in mouth to vagina contact with a female child approximately 7 years old and anal or vaginal intercourse with the child; and

6) A video dated July 14, 2015 titled 20008.wmv which is 13 minute 52 seconds in length and begins with text reading "fathers who like to touch their daughter's little pussies with fingers, tongues and cocks!" and depicts among an adult male engaging in mouth to vagina contact with a female child approximately 6 years old;

23. BEAL was interviewed by SBI SAs Heather Weber and Robert Lyons. BEAL admitted that he obtains child pornography via the Internet, and that he began downloading images and videos of child pornography in August of 2010. He further stated that he uses the Internet program Ares to search for and obtain child pornography and has previously used the program Bearshare to search for and obtain child pornography. He stated that he uses the search

term "pthc" daughter, and cumshot to obtain the child pornography files. As an investigator I am aware that "pthc", stands for preteen hardcore pornography. BEAL further stated that all the child pornography found on the hard drive at Dacobe Enterprises LLC belongs solely to him. BEAL was shown 4 images that had been downloaded from his computer by the TFO and he stated that he recognized all 4 of them as images he has previously seen and downloaded from the Internet using Ares.

CONCLUSION

24. Based upon the above information, there is probable cause to conclude that DANIEL BEAL has knowingly received child pornography using a means and facility of interstate and foreign commerce, and in and affecting such commerce, in violation of 18 U.S.C. §§ 2252A(a)(2)(A).

Special Agent Alix Skelton
Federal Bureau of Investigation

Sworn and subscribed before me
this 29th day of July, 2015.

Andrew T. Baxter
United States Magistrate Judge